UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/707,697	11/07/2000	Hong Heather Yu	9432-000112	9565

7590 06/28/2004

Harness, Dickey & Pierce, P.L.C.
P.O. Box 828
Bloomfield Hills, MI 48303

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2135	5

DATE MAILED: 06/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/707,697	YU, HONG HEATHER
	Examiner	Art Unit
	Thanhnga Truong	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *4/12/2004 (Amendment A - paper #4)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 11-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 11-18* is/are rejected.

7)☒ Claim(s) *19-21* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-4, 6-7, and 11-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Manjunath et al (US 6,332, 030)

a. *Referring to claim 1:*

i. Manjunath teaches:

(1) obtaining a first set of authentication data **[i.e., referring to Figure 15, signature image, that is "a first set of authentication data"];**

(2) said first set of authentication data being based on data contained in the first media channel **[i.e., signature data is a small fraction of host image data, the present invention can easily handle gray-scale images that could be as much as 25% of the host image (column 3, lines 20-23)];**

(3) obtaining a second set of authentication data **[i.e., data hiding speech, that is "a second set of authentication data" (column 4, line 18)];**

(4) said second set of authentication data being based on data contained in the second media channel **[i.e., a special domain embedding method for data hiding speech, that is "second set of authentication data", and video in compressed video, that is "the second media channel". is presented based on bit replacement (column 4, lines 18-21)];**

(5) hiding the first set of authentication data in the second media channel **[i.e., compared to conventional techniques, the invention can embed, that is for "hiding the first set of authentication data", significantly larger amount of signature data into the host--up to 25% of the host data, that is "the second media channel", with little or no perceptual distortion (column 4, lines 21-24)]**; and

(6) hiding the second set of authentication data in the first media channel **[i.e., compared to conventional techniques, the invention can embed/hide significantly larger amount of signature data, that is "the second authentication value", into the host, that is "the first media channel" with little or no perceptual distortion (column 4, lines 21-24)]**.

b. *Referring to claim 2:*

i. Manjunath further teaches:

(1) defining a first subset of authentication data **[i.e., referring to Figure 15, signature image, that is "a first subset of authentication data"]**;

(2) hiding the first subset in a first region of the second media channel, the first region having a first data hiding capacity **[i.e., a robust data hiding technique using channel codes derived from a finite subset of general n-dimensional lattices. In particular we use the lattice, which consists of all integer n-tuples with an even sum. As the quantity of embedded data increases, higher order shells of the lattice are included in the channel code to accommodate them. Using this approach, a gray-scale image of as much as half the size of the host image can be embedded by perturbing the host wavelet coefficients (column 3, lines 44-52)]**;

(3) defining a second subset of authentication data **[i.e., speech and video, that is "a second subset of authentication data"]**; and

(4) hiding the second subset in a second region of the second media channel, the second region having a second data hiding capacity **[i.e., a spatial domain embedding method for data hiding speech and video in compressed video is presented based on bit replacement. Spatial domain strategies are quite sensitive to transformations on the embedded signal. Compared to conventional techniques, the invention can embed significantly larger amount of signature data into the host--up to 25% of the host data, with little or no perceptual distortion (column 4, lines 18-24)].**

c. *Referring to claim 3:*

i. Manjunath further teaches:

(1) generating an identification mark for the first media channel based on a signature of the first media channel, the identification mark defining the first set of authentication data and enabling synchronization between the first media channel and the second media channel **[i.e., the signature image is one quarter the size of the host image, and both images are gray scale, one byte per pixel. Embedding occurs in the wavelet transform domain as the wavelet coefficients are combined to create a watermarked image (column 6, lines 45-48)].**

d. *Referring to claim 4:*

i. Manjunath further teaches:

(1) generating an authentication value for the first media channel, the authentication value defining the first set of authentication data **[i.e., referring to Figure 15, using DCT domain techniques and wavelet transforms to generate the signature data or authentication code, whereby such signatures include, for example, pseudo-random numbers, trademark symbols and binary images (column 2, lines 17-19)].**

e. *Referring to claim 6:*

i. Manjunath further teaches:

(1) obtaining an active data stream, the active data stream having executable content and defining the first set of authentication data **[i.e., a special domain embedding method for data hiding speech, that is "an active data**

stream", and video in compressed video is presented based on bit replacement. Compared to conventional techniques, the invention can embed significantly larger amount of signature data into the host with little or no perceptual distortion (column 4, lines 18-24)].

f. *Referring to claim 7:*

i. Manjunath further teaches:

(1) obtaining a control data stream, the control data stream further defining the first set of authentication data **[i.e., another object of the invention is to provide for including quality control in data transmission (e.g., self-enhancing images), embedding control information in audio/visual bit streams, in addition to watermarking (column 4, 27-30)].**

g. *Referring to claim 11:*

i. Manjunath further teaches:

(1) generating the first set of authentication data based on data contained in the second media channel **[i.e., referring to Figure 15, signature image, that is "a first set of authentication data"].**

h. *Referring to claim 12:*

i. Manjunath further teaches:

(1) embedding the first set of authentication data in the first media channel **[i.e., embed a significant amount of data in images, that is "the first media channel" (column 4, lines 25-26)].**

i. *Referring to claim 13:*

i. Manjunath further teaches:

(1) wherein the multimedia data stream has a third media channel, the method further including the step of hiding the first set of authentication data in the third media channel **[i.e., embedding images in audio/visual bit streams, that is "the third media channel" (column 4, lines 30-31)].**

j. *Referring to claim 14:*

i. Manjunath teaches:

(1) hiding a first subset of the active data stream in the visual channel **[i.e., visual bit streams, that is for "hiding a first subset of the active data stream" (column 4, line 30)]**; and

(2) hiding a second subset of the active data stream in the audio channel **[i.e., audio bit streams, that is for "hiding a second subset of the active data stream" (column 4, line 30)].**

k. *Referring to claim 15:*

i. Manjunath further teaches:

(1) hiding executable content in the visual channel, the executable content defining the first subset **[i.e., visual bit streams, that is for "hiding executable content" (column 4, line 30)]**; and

(2) hiding a control data stream in the audio channel, the control data stream defining the second subset **[i.e., audio bit streams, that is for "hiding a control data stream" (column 4, lines 30-31)].**

l. *Referring to claim 16:*

i. Manjunath further teaches:

(1) hiding error correction data in the audio channel, the error correction data defining the control data stream **[i.e., the MSE.sub.H (mean-square-error) is introduced into the embedded host, whereby "hiding error correction data in the audio channel" is considered to include in the MSE].**

m. *Referring to claim 17:*

i. Manjunath further teaches:

(1) hiding the first subset of the active data stream in a first region of the visual channel **[i.e., visual bit streams, that is for "hiding the first subset of the active data stream in a first region of the visual channel" (column 4, line 30)]**; and

(2) hiding the second subset of the active data stream in a second region of the visual channel **[i.e., visual bit streams, that is for "hiding the second subset of the active data stream in a second region of the visual channel" (column 4, line 30)].**

n. *Referring to claim 18:*

i. Manjunath further teaches:

(1) hiding executable content in a high capacity region of the visual channel, the executable content defining the first subset **[i.e., visual bit streams, that is for "hiding executable content in a high capacity region of the visual channel" (column 4, line 30)]**; and

(2) hiding a control data stream in a high robustness region of the visual channel, the control data stream defining the second subset **[i.e., audio/visual bit streams, that is for "hiding a control data stream in a high robustness region of the visual channel" (column 4, lines 30-31)].**

3. Claims 1 and 5-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Numao et al (US 6,512, 835 B1)

a. *Referring to claim 1:*

i. Numao teaches:

(1) obtaining a first set of authentication data; said first set of authentication data being based on data contained in the first media channel; and hiding the first set of authentication data in the second media channel **[i.e., (a) determining the j-th (j>=0) state value S_j, that is "a first set of authentication data"; (b) determining (j+1)-th state value S_{j+1} based on the j-th state value, the array element, that is "data", of the media array, that is "the first media channel", indicated by the j-th state value, and the array element of the message array; and (c) hiding data with respect to the array element of the media array indicated by the (j+1)-th state value S_{j+1} (column 3, lines 6-14)].**

b. *Referring to claim 5:*

i. Numao further teaches:

(1) calculating a one way hash value for the first media channel; and mapping the hash value onto an identification mark for the first media channel **[i.e., referring to the equation of column 9, line 25, H1 is a hash function. This K byte hashed value is used as the initial state value S.sub.0 for data hiding. The hashed value is simply used as an initial value for data hiding, so it must only**

be ensured that different outputs result from different inputs. Thus, the hashed value has no particular meaning. The operation results in the output of a value indicating the characteristics of the array, that is, the hashed value is uniquely determined on the basis of the contents of all the array elements and may depend on the contents of the overall array. If the message data is the "DATAHIDING" shown in FIG. 3(b), the output of the hash function H1 from the exclusive OR of the data indicating all the alphanumeric characters (the data in the array value m[i]) is the state value S.sub.0. The remainder if I (the number of image regions) relative to the state value S.sub.0 is the position p.sub.0. This allows the state value S.sub.0 and the position p.sub.0 to be obtained as the initial state values (column 9, lines 44-57)].

c. *Referring to claim 6:*

i. Numao further teaches:

(1) obtaining an active data stream, the active data stream having executable content and defining the first set of authentication data **[i.e., message data, that is "an active data stream" (column 21, line 44)].**

d. *Referring to claim 7:*

i. Numau further teaches:

(1) obtaining a control data stream, the control data stream further defining the first set of authentication data **[i.e., the server, that is for "obtaining a control data stream", controls the encoder so as to hide message data, that is "the first set of authentication data", in the media data read from the storage means, and transmits the output data to Internet. The above hiding method is then used to dispersively hide the message data in the media data based on the contents of the message data (column 21, lines 45-50)].**

c. *Referring to claims 8 and 9:*

i. Numao further teaches:

(1) using two dimensional checksum error correction and using multidimensional checksum error correction to generate the first set of authentication data **[i.e., the method called CRC (Cyclic Redundancy Check) can be**

used to reflect the order relationship. This algorithm is one of the algorithms for calculating check sums, and generates outputs that depend on the contents and order of the data array (column 9, lines 35-38), whereby "using two dimensional checksum error correction, and using multidimensional checksum error correction" are considered to include in this method, CRC].

Allowable Subject Matter

4. Claims 19-21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Argument

5. Applicant's arguments filed April 12, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

"Manjunath et al: teaches embedding authentication data in the video channel of the multimedia signal, and not in the audio channel or text channel."

Examiner maintains that:

It will also be appreciated that, in perceptual data hiding, one is interested in embedding and recovering high quality multimedia data, such as images, video and audio (column 2, lines 60-62).

Applicant further argues that:

"Manjunath et al. does not teach hiding authentication data representing one data channel in another data channel, and vice versa, to enable cross verification between channels."

Examiner still maintains that:

While watermarking of image data could be visible, such as a background transparent signature, a visible watermark may not be acceptable to users in some contexts. Therefore, it is preferable to digitally watermark and image by invisibly hiding a signature information into the host image, that is "hiding authentication data representing one data channel in another data channel, and vice versa". The signature is then recovered using an appropriate decoding process (column 1, lines 56-

61, see also claim 2 of Manjunath, column 24, lines 41-42). In addition, data hiding could be quite challenging if one considers embedding one image in another image, which could mean an audio signature into a host video image (column 2, lines 44-45).

Applicant further argues that:

Numao et al. does not teach hiding authentication data representing one data channel in another data channel, and vice versa, to enable cross verification between channels."

Examiner still maintains that:

Numao does teach a data hiding method of hiding media data in message data. Figure 1 is a half tone image comprising digitalized data shown on a display (see abstract). Photo description (messages) such as a "nurse", a "river", a "kindergarten pupil", and a "bird" is hidden in the media data, that is, the digitalized image in Figure 1(a), as shown in Figure 1(b), that is "hiding authentication data representing one data channel in another data channel" (column 1, lines 29-33).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

a. Yu et al (US 6,456,726 B1)discloses a data hiding system and method for providing a method of embedding multiple layers of hidden data into multimedia data (see abstract).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
June 16, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100